

Backing up your PC

Keeping copies of all your files sounds like a dull and arduous task, but Jon Thompson shows you how to do it the easy way

Your computer might have cost a lot of money, but its price pales in comparison with the value of the personal files it contains. On a home computer these probably include digital photos and video clips that are impossible to replace but are all too easy to delete or corrupt. You need to back these up or face the terrible possibility of losing them forever.

Setting up a backup routine is all well and good, but you also need to test that it works. You don't want to discover any problems after your hard disk has died and you're trying to restore your files from damaged CDs, encrypted disks or backups that require restoration software you no longer own.

Setting up a system of regular backups can be tricky and you are less likely to make copies of your files if the system is time-consuming and complex. We'll show you how to build an automatic backup system that gets on with the boring but crucial backup tasks quietly in the background, leaving you free to spend your time on fun stuff such as editing your photos and videos.

BACKUP TYPES

The most basic type of backup is the full backup. This simply means making a copy of all your files. Running a full backup every time you want to save your files is unwise, though, because it takes a long time to complete and you'll waste a lot of storage space. However, a full backup is a useful starting point for any backup strategy. Other types of backup, used in conjunction with a full backup, can dramatically cut the amount of time and effort involved.

An incremental backup copies only those files that have changed since you performed your last backup. A traditional and popular strategy for protecting data is to make one complete backup of all the data you need to preserve, and then perform regular incremental backups to save any subsequent changes.

Performed every day, incremental backups will allow you to save any new and changed files, which means you can roll back to a previous version of a file in an emergency. In practice, though, restoring a full backup followed by many incremental backups can be fiddly if you have a large stack of CDs or DVDs containing the

backup files. You'll need to restore each incremental backup in turn, which is inefficient.

You might find it more convenient to perform a full backup every few weeks, with incremental backups occurring every week or even daily. You might decide to perform a full backup every Sunday morning, for instance, and an incremental backup if required during the week, such as after downloading photos from your digital camera. To recover your system, you need only restore your last full backup followed by a few subsequent incremental ones.

Online backups provide an extra level of security because the data is stored in a different physical location to your computer. Several companies now offer secure online storage facilities that take advantage of fast broadband internet connections. See *Labs*, page 119, for our in-depth reviews of online backup services.

Some online backup services are very inexpensive. For example, BT's Digital Vault (www.digitalvault.bt.com) provides 1GB of space for free or 50GB for £4.99 a month. Storegate (www.storegate.co.uk) will keep 2GB of your data for as little as £1.49 per month, while Carbonite (www.carbonite.com) provides unlimited

INTRODUCTION

The personal data, photos, home videos and other files we store on our PCs are both priceless and, in many cases, irreplaceable. However, PCs are vulnerable to theft and damage from hackers and viruses, and they contain hard disks that can fail without warning. Just a few clumsy (or malicious) keystrokes could wipe out all your digital photos, personal videos and audio recordings.

It's crucial that you back up these files before disaster strikes, but it can be hard, tedious work. Our guide will show you how to protect your precious memories without breaking into a sweat.

Jon Thompson
IT Correspondent



contributors@computershopper.co.uk



▲ Services such as those provided by UK-based Storegate.co.uk promise to take the strain out of off-site data storage by keeping it securely online for you

Data retention Keeping your archive up to date

It's not just the physical condition of your storage media that matters. You also have to consider whether future PCs will support the hardware, file system or even the file types you use in your backup. You may think that the boffins will keep you covered, but this isn't always the case, as several high-profile mishaps have shown.

Neil Armstrong placing a foot on the Moon's surface is unarguably a high point of human achievement. The analogue tapes that recorded this giant leap are safe in the US National Archive but, until someone recently located one of the last examples of the ancient machine needed to play them, even this priceless moment in the history of our species was, in effect, lost. This isn't the only near-miss, either.

In 2003, Joe Miller of the University of South California wanted to analyse the data sent back

from NASA's breathtaking 1976 Viking mission to Mars. He discovered that the hardware for reading the tapes on which the data was stored no longer existed. He ended up having to get students to key in the data by hand from original printouts.

In the 1980s, the BBC Domesday laser disc project was supposed to mark for posterity the 900th anniversary of the original Domesday Book. By just 2002, however, it became apparent that the hardware needed to read the disc's content was already obsolete. Only software emulation and some serious reverse engineering of the data format enabled engineers to save the disc's contents.

To avoid making the same mistake, be sure to dust off your files and transfer them to a more up-to-date medium as technology evolves, or your own fading memories could be all that remain.



▲ A network storage device such as the Synology DiskStation DS-207+ can make backups easier

space for \$49.95 (around £25) per year. The advantage of these services is that you can access your files from any computer. But if the idea of storing all your personal data online makes you nervous, what are the other options?

BACKUP DEVICES

Long gone are the days when backing up meant having to use magnetic tape and expensive tape drives. The cheap availability of rewriteable CDs and DVDs means that backups don't have to cost the earth. Rewriteable optical discs are a good option because you can cycle through a small set of discs and don't have to throw away lots of used ones.

Over the past couple of years, the price of external hard disks has also fallen dramatically. Capacities have increased to the point where storing domestic backups on a separate hard disk is a viable option. Simply installing a second hard drive in the machine you need to protect is not a good idea, though. If, for instance, your computer gets a virus that runs through your drives deleting data, you could lose your backup as well as the primary copy. So, if you're going to back up to a hard disk, it's best to use a removable disk or one that's connected to another machine on the network.

For small amounts of data, a good alternative to an external hard disk is a flash memory drive. Such USB devices are now available with capacities up to 64GB. They're also cheap to buy, making them ideal for incremental backups (see *Labs*, page 111).

You could even dedicate a small server to the task of storing backups. With hardware prices falling all the time, this is becoming a viable option for homes. After all, a home server doesn't need an expensive graphics card or a fast processor. It just needs plenty of disk space.

One form of dedicated data server is the purpose-built network attached storage (NAS) server. These are essentially basic file servers that connect to your router and can be accessed from any computer on your network. Some NAS servers have two hard disks and can configure them in a RAID.

On that subject, it's time to put the record straight about RAID 1 mirroring: it won't protect your data from accidental deletion.

IT'S A RAID

RAID, which stands for redundant array of inexpensive disks, is a special type of disk

Safety net Backing up over WiFi

Wireless networks are becoming the norm in the home, but does WiFi affect your ability to save data efficiently between machines?

The way the WiFi transport protocols work, and the overheads they impose on the available bandwidth, mean you may not be getting more than a fraction of the data throughput you might expect. For each packet, all the WiFi devices on your network have to agree that it's your turn to send something. As only one packet can be sent or received at a time, congestion is a real problem if you're transferring bulk data. If your computer is grinding through a full backup of your files, which is running slowly due to network congestion, and you shut down the computer before it finishes, your

backup could be corrupt when you come to restore it after a disaster.

Performance also drops off exponentially with distance from the wireless router, so if your backup server is located in the attic and you're in the basement, you could have severe bandwidth problems. There is a solution, however.

In cases where you can't run cables between rooms, one highly efficient option is to use powerline mains adaptors. These plug into domestic mains outlets, connect to your Ethernet ports through a normal cable and act like a wired network. Some of these devices have a theoretical transmission rate of 200Mbit/s, which is fast enough for backups.

configuration that contains two or more hard disk drives. Depending on the type of RAID system you have, its controller will store your data in different ways. A RAID system can beat the problem of disk failure but nothing more. RAID won't protect you from other disasters, such as deleting a file accidentally.

In certain configurations, RAID units write the same data to all the disks they contain in a process called 'mirroring'. This ensures that if one disk in the RAID unit fails, the data can still be recovered from the others. If you have a RAID array installed in your computer, it will give you a degree of tolerance to hardware failure.

However, if you or a program on your PC deletes a file, this will be mirrored on all the disks, and your file will remain deleted just as it would if you were using a single disk drive. What's more, because of the way RAID works, you may not be able to use a file recovery utility to get your data back. With this in mind, let's take an imaginary worst-case scenario to discover what we'll need to back up.

DISASTER RECOVERY

Something terrible has happened to your computer. There's nothing for it but to use the manufacturer's rescue disc. Naturally, this will wipe the hard disk and reinstall the operating system. You're left with a pristine machine that's in the same state it was in when you first brought it home, with none of your files on it.

At this point, if you had not made a backup, you would have to go through the boring and time-consuming process of reinstalling all your applications, and then go online to let Windows Update install security updates, patches and

service packs. Most of us download and install all sorts of software that we've picked up from different places, including long-forgotten websites and magazine cover discs. Replacing these programs can be practically impossible, but not as impossible as replacing the data you have lost.

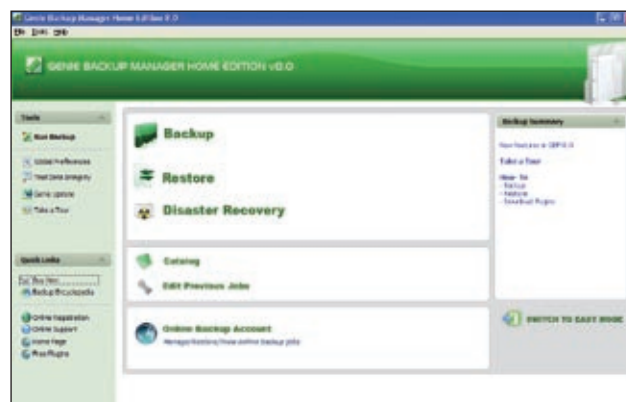
Luckily, you did make a backup, so the only thing you need to install on your pristine system is your backup software. Once this is loaded you can instruct your PC to begin restoring your backups, after which all your applications, commercial and obscure, will be available. You would start by restoring the last full backup you made of your data, followed by the small set of incremental backups you made after that. The only question left is how to make those backups with the least fuss.

SAFE AND SOUND

Once you have backed up your data, what next? If it's on a server, you should copy it to a removable device or discs for complete safety. Simply putting this secondary backup in a drawer isn't really good enough to protect it in the long term, however. If there were a fire, you could still lose everything, so you need to find a better place to store it.

One idea is to buy a little fire safe. Aim for a safe with a rating of an hour or more of fire protection. While it might seem expensive, a good-quality fire safe isn't just for your backup media. You can store other information, such as your insurance policies, which are handy things to have around if you've just had a fire.

Offsite storage is also a good idea. It might be as simple as dropping off and collecting a



◀ Genie Backup Manager Home Edition 8.0 by Genie-Soft is an ideal, low-cost, domestic backup solution

HOW TO... Back up your PC automatically

There are plenty of advanced commercial backup utilities on the market, but to get you started and into the habit of protecting your data, we're going to show you how to use the inexpensive (\$49, around £25), easy-to-use Genie Backup Manager Home Edition from Genie-Soft (www.genie-soft.com).

You may be wondering why we don't use the backup program built into Windows. Sadly, Microsoft Backup has some fundamental problems that make it less than ideal, including an inability to back up directly to optical media. If you back up to a hard disk it will attempt to overwrite the previous backups, which you don't want. Although it will prompt you about this, and give you an opportunity to rename the backup, this spells doom for automating the backup.

There is also a subtle difference between the versions of Microsoft Backup that come with Windows XP Pro and Home editions. The Home edition doesn't have the Backup program installed by default and, although you could always dig out the Windows installation CD, we don't advise using it because it doesn't support Automatic System Restore (ASR) – despite giving no clue to this limitation.

1 Run Genie Backup Manager and you'll be greeted by the main page, which provides options for Backup, Restore and Disaster Recovery. Click on the Backup option to begin a new backup job. Down the left-hand side of the second screen you'll see a list of steps. This first step concerns collecting backup job information. Select the radio button next to the option to make a new backup. Now enter a name and a description and press the green Next button at the bottom right of the screen. You can use the back button at any time to return to a previous step without losing any settings.

2 Select a destination for your backup. Unlike Microsoft's backup utility, Genie Backup Manager allows you to make backups directly to optical media, over FTP to a remote server and even directly to an online backup service. The software also allows you to use all available space on rewritable media or reserve some for other purposes. It can format rewritable media too, and will automatically split your backup across multiple disks, prompting you to insert a new one when the time comes.

3 Next we need to select the files to back up. Genie splits this task between three tabs, called My Profile, My Folders and My Plugins. The first enables you to save your data from applications such as Outlook, other email clients, the Registry, the fonts folder and other traditionally tricky areas. The My Folders tab lets you back up the My Documents folder structure, as well as other areas. The final tab lets you back up operating system plug-ins, such as WinZip.

It may not make sense to back up every file on your computer. If you capture video footage from a DV camcorder, for example, you may have enormous files of over 2GB. These will eat up your backup storage space. As long as you make a policy not to reuse or wipe your DV tapes, you already have a backup of your video footage. You'll have to re-capture it to your hard disk if disaster strikes your PC, but you will save time in the long run.

4 Genie Backup Manager supports full and incremental backups. If you back up to a

EXPERT TIP

Use disk-imaging software instead of a traditional backup program, and you will be able to restore your PC to exactly how it was quickly and easily. Norton Ghost and Acronis True Image are good choices.

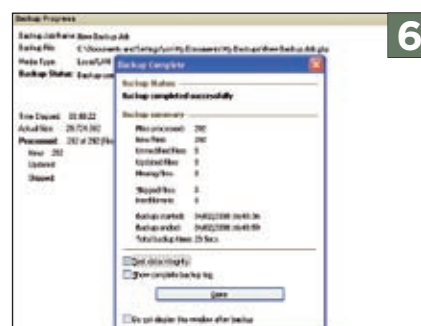
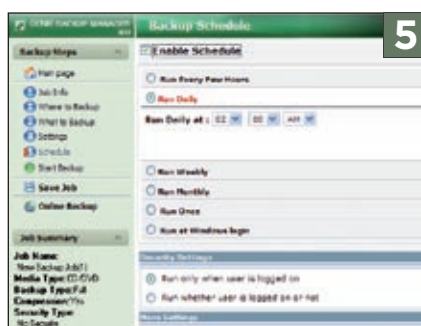
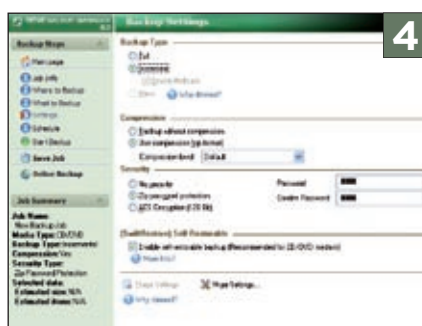
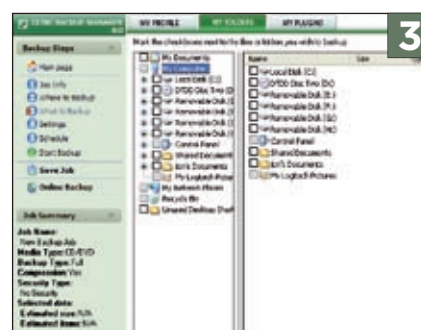
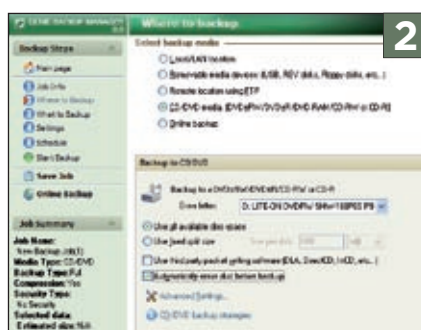
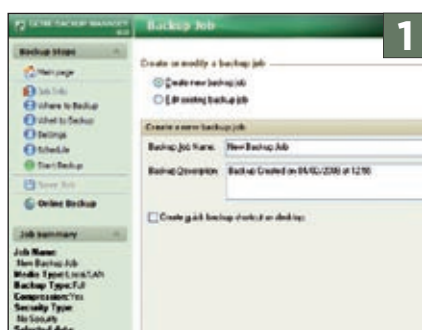
blank disc, it will automatically create a full backup of the areas you've selected, even if you've selected an incremental backup. If the disc already contains a full backup, it will add the incremental backup to it. A very useful option here is Zip compression, which saves space. You have a choice of compression levels, with higher compressions being slower. The

SwiftRestore option will create the backup as a .exe file. To restore it on any machine, you simply double-click the archive. For better security, enter a password to protect the archive before moving to the next step.

While incremental backups can save space and time, you should consider creating a fresh, full backup regularly. By doing so you can restore your system quickly, without having to find and load lots of discs containing the previous incremental backups.

5 For the final step you will see a pop-up window asking if you want to begin the backup now, schedule it for later or save the job to run manually later. If you select the schedule option, a further step appears. You can now select to run your schedule daily, weekly, monthly, at bootup and once. You can also run the backup every few hours, which is useful for a system that changes constantly. Making backups really doesn't get much simpler than this.

6 Once a manual backup is complete, you will see a pop-up window telling you the outcome. A tick box for testing the backup's integrity appears once it has finished. Use it and, when you press Done, the software will verify the archive. This is a good idea for avoiding the unwelcome situation of having backups that you can't restore later.



USB flash drive when you visit a relative, or keeping it at the office. The critical thing is that the backup is geographically separate from the live data. If you have a secure facility to hand, such as a locked shed or garage, hiding it in there can be a good idea.

BACKUPS FOR LIFE

How long will your backups last if you simply place them in a cool, dry, safe place and forget about them? This is not as strange a question as you might think, because digital media does degrade over time.

Although CDs were introduced in the early 1980s with demonstrations of their indestructible nature, over time they react to the moisture and grease they encounter when handled. This can eventually eat into their surfaces. Scratches, even very tiny ones, are also

a problem for some low-cost brands. You can try to recover a scratched disc using a CD or DVD polishing kit, but it should be your last resort, so it pays to buy branded media.

Even the lifespan of modern flash memory is being brought into question now that it has been around for a while. Like other digital data storage devices, flash memory incorporates extensive error checking, but there comes a point where there's not enough data left to correct and it is lost forever. Because of this, if you're storing data for the long term, it's essential that you test it for readability every once in a while.

Some backup programs can also encrypt their backups. As new security algorithms become available, it's essential that you don't forget to restore and re-create your long-term backups using newer encryption schemes. What may seem standard now may not be in ten or more years' time. If the encryption scheme requires a password, it's very important that you store this in a safe place, too.

When you upgrade to new hardware, it's essential that you still have a means of restoring your backups to the new machine. Data stored on floppy disk is already unreadable in many modern systems. One day DVD media will be obsolete, so if you have a photographic archive of your life that you'd like to be able to share with your grandchildren in the distant future, you must keep that archive in a format that next-generation machines will be able to read. You need to recreate your archives on new media over the years as new media technologies become available. This will also give you the opportunity to check that the media you're upgrading from isn't so old that it has degraded way past the point of recovery.

WINDOWS HOME SERVER

For many households, running a dedicated backup server is becoming an increasingly attractive option. Microsoft has recognised this

fact and produced Windows Home Server. This operating system is designed to run on a dedicated server that acts as a central data hub for your home network, including PCs, networked Xbox 360 games consoles and other devices. The idea is partly to share data, but that's not all.

Windows Home Server comes with a software client that you install on the other Windows machines on the network. This enables the server to back them up automatically each night, and gives you the ability to restore a machine quickly if it fails, as well as providing access to individual files. The client software also allows the server to monitor the health of other machines on the network and to alert you to any problems.

One useful feature of Windows Home Server is that it enables you to contact your server securely from anywhere in the world. This is useful if, for instance, you're on holiday and the memory card in your camera becomes full. You can download the images to the server and keep snapping. Your photos will also be safe even if someone steals your camera.

For those with shallower pockets and more modest needs, an alternative to a full-blown Windows Home Server is a computer running Linux and the open-source Samba. Samba is bundled with most mainstream Linux distributions, and lets you share the server's disk space with Windows systems.

STAY SAFE

It's a fact of life that even people who wouldn't dream of working on a note for the milkman without hitting the save button every few seconds balk at making backups of the data they really can't afford to lose. But increasingly, the data we risk losing is emotionally very precious. Making backups needn't be a chore. A few minutes a week is all it takes to keep you safe from a variety of threats. **CS**



▲ Microsoft's new Windows Home Server could become an important part of household networks

HOW TO... Restore your files

If disaster strikes your computer, you'll need to restore your files from your backups. Here's how.

1 To restore files from a previous backup, open Genie's main page and click on the Restore icon. This brings up a catalogue of all your completed backup jobs, under which will be

individual entries for each 'run'. Expand a job entry to display the backup runs it contains. Select a backup and press the Next button.

2 You should now see a list of files in the backup. You can either select individual areas to restore or click the first

box to choose the entire set of files. Then click the Next button to continue.

3 The final screen in the restoration process confirms that you want to start restoring files. Press Restore Now and the files will be restored. That's all there is to it.

